SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Konrad Adenauer Stiftung

9th Berlin Conference on Asian Security (BCAS)

International Dimensions of National (In)Security
Concepts, Challenges and Ways Forward

Berlin, June 14-16, 2015

A conference jointly organized by Stiftung Wissenschaft und Politik (SWP), Berlin and Konrad-Adenauer-Stiftung (KAS), Berlin

Discussion Paper
Do Not Cite or Quote without Author's Permission

Session III: Cyber Security

Elina Noor
Institute of Strategic and International Studies (ISIS)
Kuala Lumpur

International Dimensions of National (In)Security Concepts, Challenges and Ways Forward: Cyber Security

Elina Noor

Over the last decade, awareness among ASEAN member states of the need to secure cyber space has matured from a cursory acknowledgement of the urgency to increased recognition of, if not, actual protection planning of critical infrastructure. Much of the focus surrounding cyber space since the early 2000s, however, has remained on content and information security. Declarations and communiques on cyber-crime and online radicalization featured conspicuously in the aftermath of the 11 September 2001 terrorist attacks in the United States. These and other related initiatives have been reinvigorated in recent times with the resurgence of violent extremism radiating outwards from Syria and Iraq to other parts of the world. Additionally, real and perceived challenges posed by social media to the political stability of a state and government posed have gradually emerged as serious concerns within South East Asia.

As ASEAN edges closer towards consolidation as a Community by the end of this year with greater integration as an enduring, post-2015 goal, the connectivity agenda that anchors many of the region's plans for networks of roads, railroads, ports, and flight corridors remains geared towards physical infrastructure. For reasons such as differing levels of technological development and priority, there has been less emphasis on digital connectivity and even less on the framework of regulations and laws to underpin it. To be sure, Southeast Asia remains the most advanced developing region in implementing e-commerce laws. It was the first to adopt a harmonized legal framework for e-commerce in the developing world. Nine of the 10 ASEAN countries have laws related to electronic transactions while eight have laws concerning cybercrime. This is perhaps unsurprising given that economic prosperity has always been a priority for the maintenance of political and regional stability since the institutionalization of ASEAN.

What is missing, however, is a concerted conversation on the interaction of states – in this case, neighbouring states that along with their dialogue partners have acceded to the Treaty of Amity and Cooperation – in cyber space and the extent to which international law applies in the event of an attack in this emerging domain. The latter half of the question is fraught with definitional issues, implications, and consequences. Yet, while other states – including ASEAN’s Notheast Asian neighbours – debate these hotly, the silence from Southeast Asia has been resounding.

Under the current framework of international law, a state that suffers an armed attack from another is afforded recourse to self-defence measures. It is as yet unclear - despite declarations by some states and the 2013 UN Group of Governmental Experts' (GGE) statement to the effect - whether the exact same provisions and scope are available in the event of a cyber-attack. One encouraging product of the UN GGE report, however, was the acknowledgement of the applicability of international law – writ large – particularly the UN Charter to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment.

Despite the enormity of the matter and its implications for all states, discussion on this matter is being advanced predictably and only by a few countries in the developed world. The Tallinn manual - an extraordinary initial initiative to make sense of the relationship between cyber space and international law - regrettably did not involve any independent experts from Asia. Absent other comprehensive efforts, the manual will likely be the base for clarifying the state of play and rules of engagement on cyber space. The future may be in Asia but the sun seems to have yet to rise in the East in cyber space.

ASEAN member states have traditionally avoided even talk of conflict. But as these countries become increasingly inter-dependent not only among themselves but with their regional neighbours, greater trust will need to be built to collaborate at the strategic level in cyber security before norms and rules overtake, or are superimposed, upon them from beyond the region.

Additionally, whereas technical experts have few problems sharing and working cooperatively, strategic sensitivities and suspicions will somehow need to be talked through to facilitate a similar level of exchange among security and military agencies where cyber commands or structures are usually parked within nations.

As ASEAN countries become increasingly dependent on the Internet and each other as a Community, a coordinated, strategic, and long-term approach to cyber security needs to be individually and jointly developed beyond the narrow confines of a trade/economics or transnational crime focus. Even the ASEAN Political-Security Community Blueprint places cyber security within these contexts rather than anticipating how evolving threats may impact upon fundamental precepts like state sovereignty and international law.

Several recommendations follow. First, because strategic cyber security draws on effective coordination beyond the technical, increased discussions and exchanges will need to take place among stakeholders in law, diplomacy, and politics at tracks 1 and 2. Strategic cyber security, after all, draws on a cooperation and collaboration of various skill-sets drawn from diplomacy, politics, and law. Cyber-attacks against a

state's critical national infrastructure – however that may be defined – should be guided by an informed policy umbrella beyond an exclusively technical lens.

Second, national cyber security strategies provide a good foundation to expand upon considering the role of the state, in concert with other relevant domestic stakeholders, in crafting the framework for cyber operations. This is significant given that the state is the primary arbiter of peace and security in the physical - and arguably, virtual - domain.

Third, in order to improve responses to cyber-attacks; advance clarity of intention, and action; and promote transparency, confidence, and trust among countries, table top exercises and simulations should increasingly be added to existing joint military exercises or training. At the regional level, these could be held on the sidelines of ADMM or ADMM Plus meetings. The same concept of military interoperability that affords seamless coordination among the forces of different states should be replicated in the virtual realm so that decisions and actions can be synchronized as best as possible in the event of a major cyber-attack. With the infrastructure of cyber space stretching across borders, in the seas and in the clouds, the possibility of consequences spilling over into neighbouring countries in an integrated ASEAN Community should be an even more urgent catalyst for closer cooperation within the region. A greater number of exercises and simulations involving cyber space should therefore increasingly be the norm.

Fourth, to reduce the public/private sector dichotomy particularly in South East Asia, the private technology sector should be included and consulted more frequently in policy discussions concerning cyber space. Similarly, having public sector policy representation at private sector roundtables, seminars, or workshops would help both sides understand each other's perspectives. Specifically, Tracks 1 and/or 2 could, together with the private sector, jointly organize simulations at IT security conferences or policy roundtables within the region to raise awareness of the technical challenges of cyber security as well as the overarching policies to guide cyber operations. This cross-pollination of views would help sensitize both sides to the roles of, and initiatives taken, by the other side. This would be particularly helpful in Southeast Asia given that the strategic and defence technology is more nascent than in Northeast Asia where there is also a less pronounced public/private sector dichotomy in related sectors. Within a nascent cyber security landscape such as Southeast Asia's, incorporating private sector perspectives into government decisions would streamline and fast-track the harmonization of public/private sector efforts from the beginning.

Fifth, given the political sensitivities surrounding cyber security, there is a role for Track 2 institutions to take the lead where Track 1 is unable or unwilling to. This has

at least three advantages: (i) Track 2 is able to draw representation from among diverse expert stakeholders within and outside of government without the formalities accompanying Track 1; (ii) Track 2 is typically known for its frank and candid discussions without attribution to national positions; and (iii) Track 2 is able to stitch (i) and (ii) together to offer policy recommendations cognizant but unbound by the political constraints clouding government discussions.

The rules for state behaviour in cyber space and that of entities under their authority are an extension of the international legal framework governing inter-state relations in the real world. A clear national position within Southeast Asia on these matters would greatly clarify interactions at the regional and international level.